CERTIFICATION AND ACCREDITATION - PROCESSES AND LESSONS LEARNED

Chair: Mr. Jack Eller, DISA, CISS (ISBEC)

Panelists: Paul Wisniewski, National Security Agency

Candice Stark, Computer Sciences Corporation

Ray Snouffer, National Institute of Standards and Technology

Barry C. Stauffer, CORBETT Technologies, Inc.

Panel Summary

Mr. Jack Eller, DISA
CISS (ISBEC)
701 South Courthouse Rd.
Arlington, VA 22204-4507
(703) 681-7929, ellerj@ncr.disa.mil

On August 19, 1992 the Office of Assistant Secretary of Defense directed the Defense Information Systems Agency (DISA) Center for Information Systems Security (CISS) to formulate a standard DoD process for security certification and accreditation. CISS formed a working group, consisting of Service and Agency representatives. The working group evaluated ten existing processes, but found none which could be adopted Department of Defense (DoD)-wide. As a result, the working group developed the DoD Information Technology Security Certification and Accreditation Process (DITSCAP). A uniform process across DoD, DITSCAP applies to accreditation of both strategic and tactical systems, as well as stand-alone information systems or networks. DITSCAP capitalized on approved security techniques, software, and procedures to reduce the complexity and overall cost of the accreditation process. The DITSCAP integrates security directly into the system life cycle and is designed so that it can be applied uniformly across DoD. The DITSCAP defines a process which standardizes all activities leading to a successful accreditation, thereby minimizing the risks associated with nonstandard security implementations across shared Defense Information Infrastructure (DII) and end systems. The DITSCAP has been designed to support the requirements of Office of Management and Budget Circular A-130.

In contrast to the prevailing system based accreditation processes, the DITSCAP is focused on the infrastructure and views systems and networks as components of the infrastructure. The view of the DITSCAP, therefore, differs from such documents as the National Computer Security Center (NCSC) Certification and Accreditation Process Handbook for Certifiers (NCSC-TG-031). CISS and the NCSC have agreed that for the near term, NCSC-TG-031 provides sound

guidelines. DITSCAP provides the midterm and long term infrastructure-centric approach to the security certification and accreditation of systems and networks. These two processes have been harmonized to reflect the transition to the DITSCAP. Both terminology and structural parallels will facilitate a smooth transition between these two processes.

Our panelists today will present an overview of the elements and approval status of the Certification and Accreditation Process Handbook for Certifiers, an the Certification and Accreditation Process Handbook for Accreditors. Following these presentations we have two presentations which will discuss some lessons learned in applying each of the two processes.

THE CERTIFICATION AND ACCREDITATION PROCESS HANDBOOK FOR CERTIFIERS

Paul Wisniewski
National Security Agency
Office of Commercial Programs and Enabling Technologies
9800 Savage Road
Ft. Meade, MD 20755-6740
(410) 859-6281, pawoeck@radium.ncsc.mil

The National Computer Security Center is publishing the *Certification and Accreditation Process Handbook for Certifiers* as part of the "Rainbow Series" of documents. This document continues the series on certification and accreditation (C&A) and provides the certifier and accreditor with a structured process to perform a C&A of a system. It should be viewed as guidance in determining the amount of effort and the resources necessary to certify and accredit a system. As technology that supports the infrastructure of automated systems becomes more sophisticated, the C&A process will, no doubt, require new or additional guidance. However, this document provides the necessary certification and accreditation guidance for now and into the near future.

The terminology and structure in the *Certification and Accreditation Process Handbook for Certifiers* has been harmonized with the *DoD Information Technology Security Certification and Accreditation Process (DITSCAP)*. Thus DoD elements may use this document in support of their C&A requirements. However, this document is not DoD specific. The C&A process described is consistent with the earlier guideline, *Introduction to Certification and Accreditation*. Non DoD agencies and organizations should have few problems in seeing the parallels and using this latest document to support their C&A programs.

The purpose of this handbook is to establish a standard approach for performing C&A on systems regardless of the acquisition strategy or life-cycle status. This handbook provides guidance about the C&A process based on the degrees of assurance required and other factors related to a system. Assurance is a measure of confidence that the security features, attributes, and functions enforce the security policy. Assurance refers to the claims for evidence for believing the

correctness, effectiveness, and workmanship of the security service or mechanism. Certification verifies and validates the security assurance fora system associated with an environment. Accreditation evaluates whether the operational impacts associated with any residual system weaknesses are tolerable or unacceptable. The degrees of assurance assumed by a development team, certification team, or Accreditor about a system reflect the confidence that the system is able to enforce its security policy correctly during use and in face of attacks.

The C&A process allows the DAA, Program Manager, and User representative to tailor the certification efforts to the particular system mission, threats, environment, degrees of assurance, and criticality of the system, as necessary, as long as they comply with network connection rules. With a standard approach established, reuse of both the technical and nontechnical analyses from the certification effort , for recertification or certification of a similar system, might be possible. The C&A process should encourage and preserve commonality in understanding, be consistent in application, be open to evolution and growth, employ feedback, and be applied continuously. This process should be scalable to the size of the system, repeatable, and predicable.

STANDARDS IN CERTIFICATION AND ACCREDITATION

Candice Stark
Computer Sciences Corporation
7471 Candelwood Road
Hanover, MD 21076
(410) 684-6329

This presentation will address the why, who, what, how and where of C&A standards. The speaker will expand on the latest in the Rainbow series C&A sub-series, the Accreditor's Guide. Ms. Stark was initially immersed in C&A while at NSA. While there she was intimately involved with the creation/editing of the three C&A documents in the Rainbow series. Now at CSC, she is still involved in C&A issues for the DoD.

THE CERTIFICATION OF THE INTERIM KEY ESCROW SYSTEM

Ray Snouffer
National Institute of Standards and Technology
Building 820, Room 414
Gaithersburg, MD 20899
(301) 975-4436, ray.snouffer@nist.gov

The U.S. Government Key Escrow System (KES) provides for lawfully authorized access to the key required to decipher communications secured with products built in conformance with the Escrowed Encryption Standard, Federal Information Processing Standards Publication (FIPS) 185. This paper is intended for presentation at the 1996 National Information Systems Security Conference. The purpose of this paper is to describe the certification and accreditation of the Interim KES and provide an historical overview of the Key Escrow Certification Working Group's (KECWG) activities. The defined purpose of the certification working group is to perform a certification on both the interim and the final KES in accordance with the Guideline for Computer Security Certification and Accreditation (FIPS 102). FIPS 102 provides guidelines for computer security certification and accreditation of sensitive computer security applications. The National Institute of Standards and Technology (NIST) chairs the KECWG. In addition to NIST, the membership consists of the Department of Justice (DOJ), the Department of Treasury, the Federal Bureau of Investigation (FBI), the National Security Agency (NSA) and the Department of Commerce (DOC).

LESSONS LEARNED FROM APPLICATION OF THE DEPARTMENT OF DEFENSE INFORMATION TECHNOLOGY SECURITY CERTIFICATION AND ACCREDITATION PROCESS (DITSCAP)

Barry C. Stauffer
CORBETT Technologies, Inc.
228 N. Saint Asaph Street
Alexandria, VA 22314-2517
(703) 519-8639, staufferbc@aol.com

The DITSCAP establishes a standardized process, set of activities, general task descriptions, and a management structure to verify, validate, implement and maintain the security posture of the DII. The DITSCAP is designed to be adaptable to any type of Information Technology (IT) and any computing environment and mission. It can be adapted to include existing system certifications and evaluated products. It can use new security technology or programs, and adjust to the appropriate standards. The process may be aligned with any program acquisition strategy. Its activities can be integrated into the system life cycle to ensure the system meets the accreditation requirements during development and integration and continues to maintain the accredited security posture after fielding. While DITSCAP maps to any system life cycle process, its four phases are independent of the life cycle strategy. The DITSCAP's, four phases, Figure 1, are: Definition, Verification, Validation, and Post Accreditation.

- Phase I, **Definition**, defines the Certification and Accreditation Level of Effort, identifies the Designated Approving Authority, and documents the security requirements necessary for the certification and accreditation in a single document, the System Security Authorization Agreement (SSAA). Phase I focuses on understanding the mission, environment, and architecture to determine the security requirements and level of effort necessary to achieve accreditation.

- Phase II, **Verification**, verifies the evolving, or modified, system's compliance with the agreed upon security requirements.

- Phase III, **Validation**, validates the fully integrated system's compliance with the security requirements. Phase III concludes with full approval to operate the system, e.g., security accreditation.

- Phase IV, **Post Accreditation**, monitors system management, operation, and maintenance to preserve an acceptable level of residual risk. Phase IV includes those activities necessary for the continuing operation of the accredited system, e.g. change management, security management, and periodic compliance validation.

Phases I, II, and III are the DITSCAP process engine. The DITSCAP methodology permits the forward or backward movement between phases to keep pace with the system development or to resolve problems. Therefore the phases are repeated as often as necessary to produce an accredited system. The objective of these steps is to achieve agreement between the Program

Manager, DAA, and the Users Representative at each step of the process.

The DITSCAP was used as the basis for the certification and accreditation process in a recent government client server environment involving over 500 workstations. The application processes sensitive but unclassified information. This C&A effort was designed to meet the requirements of the new OMB A-130 Appendix III.

This presentation will discuss some of the lessons learned in the application of this new process. The discussion will include project planning, system analysis, requirements definition, requirements tracing, test planning, and testing.